Esclarecendo a defesa LINA da ameaça de FirePOWER processe a utilização CPU

Índice

Introdução

P: Por que o processo de Lina na defesa da ameaça de FirePOWER consome 100% (ou mais) CPU?

R: Isto é normal porque o processo de Lina está votando constantemente o Network Interface Cards (NIC) para o tráfego de entrada. Em curto, a utilização do processo de Lina pode com segurança ser ignorada.

Contribuído por Mikis Zafeiroudis, por Ignacio Penalva, por Haitham Jaradat e por David Torres Rivas, engenheiros de TAC da Cisco.

Análise

A defesa da ameaça de FirePOWER é um sistema operacional unificado que consiste em 2 motores (ASA e Snort).

O FTD CLI mostra que o processo de “Lina” (motor ASA) consome muitos ciclos de CPU. Está aqui um exemplo de um FTD que é executado no dispositivo ASA5506-X:

```
> system support utilization
top - 01:26:40 up 12 days, 16:00,  1 user,  load average: 22.08, 22.10, 22.10
Tasks: 161 total,   1 running, 159 sleeping,   0 stopped,   1 zombie
Cpu(s): 22.6%us,  4.1%sy,  0.0%ni, 73.2%id,  0.1%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   3927684k total,  2793860k used,   120904k free,   181548k buffers
Swap:  3996668k total,   257632k used,  3739036k free,   831372k cached

 PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
23000 root       0 -20 1138m 513m  91m S   99 13.4  18205:20 lina <--
 2952 admin     20   0 15240 1156  848 R    2  0.0   0:00.02 top
22941 root      20   0  266m 2316 2108 S    2  0.1  47:16.70 ndmain.bin
   1 root      20   0  4232  652  620 S    0  0.0   0:12.40 init
```

Na saída acima você deve realmente tomar-nos na consideração (usuário) + utilização CPU sy

(do sistema) junto com o valor identificação (quietude - não usada).

Éaqui de um FTD ser executado no dispositivo do FPR-9300:

```
> system support utilization
top - 04:30:22 up 40 days,  5:22,  0 users,  load average: 26.12, 26.10, 26.13
Tasks: 568 total,   1 running, 566 sleeping,   0 stopped,   1 zombie
Cpu(s): 22.1%us,  0.2%sy,  0.0%ni, 77.6%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:  264374828k total, 28976700k used, 234868048k free,      268k buffers
Swap:        0k total,        0k used,        0k free,   529812k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
12772 root       0 -20 24.8g 541m  88m S 1593 0.2 927288:05lina <--
12594 mysql     20   0 3063m 150m 9140 S    4  0.1  56:28.39 mysqld
12608 root      20   0 24696 2848 1192 S    2  0.0 422:45.07 pdts_proc
43145 admin     20   0 15648 1484  844 R    2  0.0   0:00.01 top
    1 root      20   0  4232  632  552 S    0  0.0   0:15.43 init
```

Recomendações

- Do “a utilização suporte de sistema” ignora na utilização do processo de “Lina”.
- Para monitorar a utilização CPU FTD verifique valores “nós " + " identificação SYS " + "”
- Em relação à monitoração do motor ASA você deve verificar as seguintes saídas:

Saída 1

```
> show cpu usage
CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%
```

Saída 2

```
> show processes cpu-usage sorted non-zero
PC                  Thread               5Sec     1Min     5Min   Process
0x00007f42428f1fd9  0x00007f42290b9ea0    0.2%     0.0%     0.0%   ci/console
```